Systematic Maximum Sum Rank Codes

Paulo Almeida, Umberto Martínez-Peñas and Diego Napp

Paulo Almeida Dept. of Mathematics, University of Aveiro, Portugal, palmeida@ua.pt
Umberto Martínez-Peñas, Dept. of Electrical & Computer Engineering, University of Toronto, Canadaumberto@ece.utoronto.ca
Diego Napp, Dept. of Mathematics, University of Alicante, Spain, diego.napp@ua.es

Abstract

In the last decade there has been a great interest in extending results for codes equipped with the Hamming metric to analogous results for codes endowed with the rank metric. This work follows this thread of research and studies the characterization of systematic generator matrices (encoders) of codes with maximum rank distance. In the context of Hamming distance these codes are the so-called Maximum Distance Separable (MDS) codes and systematic encoders have been fully investigated. In this paper we investigate the algebraic properties and representation of encoders in systematic form of Maximum Rank Distance (MRD) codes and Maximum Sum Rank Distance (MSRD) codes. We address both block codes and convolutional codes separately and present necessary and sufficient conditions for an encoder in systematic form to generate a code with maximum (sum) rank distance. These characterizations are given in terms of certain matrices that must be superregular in a extension field and that preserve superregularity after some transformations performed over the base field. We conclude the work presenting some examples of Maximum Sum Rank convolutional codes over small fields. For the given parameters the examples obtained are over smaller fields than the examples obtained by other authors.

Keywords: Maximum Rank Distance, Maximum Sum Rank Distance, Convolutional codes, Superregular matrices, Gabidulin codes

1. Introduction

Maximum Distance Separable (MDS) codes are block codes whose minimum Hamming distance attains the Singleton bound. In the linear case, they are characterized by having a generator matrix $G \in \mathbb{F}_q^{k\times n}$ whose full size $k \times k$ minors are all nonzero, where $k < n$ and $\mathbb{F}_q$ is a finite field. If G is in systematic form, *i.e.*,

$G = [I_k \ P]$, where I_k is the identity matrix of size k, then, the MDS property can be characterized only in terms of the matrix P, namely, all minors (of any size) of P must be nonzero. One well-known example of this class of matrices is the set of generalized Cauchy matrices [4], which correspond to systematic generator matrices of Reed-Solomon codes [17].

In the last decade, rank-metric codes have been a very active area of research due to their wide range of applications in reliable and secure linear network coding [14], postquantum cryptography [11], local repair in distributed storage [32] and space-time coding [16]. Block codes attaining the Singleton bound for the rank metric are called maximum rank distance (MRD) codes. Unfortunately, if one represents such codes as subsets of $\mathbb{F}_{q^M}^n$ with ranks defined over $\mathbb{F}_q$, then all known MRD constructions (e.g., [6]) are only decodable in superlinear time in n over $\mathbb{F}_{q^M}$, where $M \geq n$ (thus q^M is exponential in n), and achieving linear-time decoding is already an extremely hard problem even in the Hamming metric. Thus it seems that MRD block codes will hardly ever be practical in real applications.

Recently, the sum-rank metric, which simultaneously extends the Hamming and rank metrics, has gained interest in the area. It was implicitly considered for multiple fading blocks in space-time coding [16, Sec. III], and then formally introduced for multishot network coding [19, 23, 26, 35]. The sum-rank metric, in the form of column rank distances, is the natural metric for convolutional codes tailored for streaming over linearly coded networks [26, 19]. The problem of constructing convolutional codes with maximum column (Hamming or rank) distances has attracted a lot of attention in recent years [2, 3, 8, 9, 15]. In the Hamming context, it was shown in [8] that the construction of convolutional codes with optimal column distances boils down to the construction of lower (block) triangular Toeplitz superregular matrices (see the formal definition in Section 2). Several results on superregular matrices have been recently presented in [2, 3, 9, 15, 27]. However, over small fields only constructions of superregular matrices with small parameters have been presented, most of them found by computer search. General constructions have also been presented, but require unpractical large finite fields [1, 8], e.g., doubly exponential.

On the other hand, block codes equipped with the sum-rank metric are also of interest for reliable and secure multishot network coding [23] and especially for local repair in distributed storage [24]. This is due to linearized Reed-Solomon codes [21], which are the only known MSRD (maximum sum-rank distance) block codes with subexponential field sizes for decoding, in contrast with MRD block codes which are practical only for moderate parameters (see [23, Table I] and [24, Section VI]).

In this work, we give sufficient and necessary conditions for linear block and convolutional codes to be MSRD only in terms of the matrix $P \in \mathbb{F}_{q^M}^{k\times(n-k)}$ (resp.

$P(D) \in \mathbb{F}_{q^M}^{k\times(n-k)}[D]$), when the generator matrix of the code is in systematic form, *i.e.*, $[I_k \;\; P]$ (resp. $[I_k \;\; P(D)]$). For consistency with the convolutional literature, we will use the terms encoder and generator matrix interchangeably. These conditions will require not only that all the (non-trivial) minors of P (resp. $P(D)$) are nonzero, but that they remain nonzero after some operations over the base field $\mathbb{F}_q$. Worth mentioning is the thorough work in [28, 29] on systematic encoders of block MRD codes and the family of generalized Gabidulin codes. This class of codes are the rank analogue of the generalized Reed-Solomon codes and their nonsystematic encoders are given by s-Moore matrices, the q-analogues of weighted Vandermonde matrices. We note that MRD codes are q-analogues of MDS codes, but MSRD codes are not.

The outline of this paper is as follows. In Section 2, we present fundamental preliminary results on the structure of rank codes, convolutional codes and superregular matrices. In Section 3, we address and present first a matrix characterization for a systematic block code to be MRD and MSRD. We then proceed to tackle the more involved characterization of systematic convolutional codes with optimal column rank distances. We also address the general case of a convolutional code that does not necessarily admit a systematic polynomial encoder. The last section is devoted to present concrete examples of optimal codes over relatively small field sizes which improve the existing examples in the literature.

2. Preliminaries

In this section, we present the setting and necessary results to address the problems in the remainder of the paper.

2.1. Block codes

A block code is simply a nonempty subset $\mathcal{C} \subseteq \mathbb{F}_{q^M}^n$, which we will consider to be $\mathbb{F}_{q^M}$-linear from now on. In case its dimension is k, we call it an (n, k) code. Let $M_n : \mathbb{F}_{q^M}^n \longrightarrow \mathbb{F}_q^{M\times n}$ denote the $\mathbb{F}_q$-linear vector space isomorphism that expands every scalar in $\mathbb{F}_{q^M}$ as a column vector in $\mathbb{F}_q^M$, with respect to some basis. Then we may define the rank metric in $\mathbb{F}_{q^M}^n$ by $d_{\mathrm{R}}(v, w) = \mathrm{rank}(v - w)$ (see [6]), where $\mathrm{rank}(v) = \mathrm{rank}(M_n(v))$, for all $v, w \in \mathbb{F}_{q^M}^n$. In this context, codes are sometimes considered as subsets of $\mathbb{F}_q^{M\times n}$ to use matrix operations or to restrict the study to $\mathbb{F}_q$-linear codes.

The rank metric admits a natural extension, called sum-rank metric. If we partition the code length $n = n_1 + n_2 + \cdots + n_\ell$, then we may define the corresponding

sum-rank metric (see [16, 21, 22, 26, 35]) as

$$d_{\mathrm{SR}}(v,w) = \sum_{i=1}^{\ell} d_{\mathrm{R}}(v_i, w_i) = \sum_{i=1}^{\ell} \mathrm{rank}(M_{n_i}(v_i - w_i)), \tag{1}$$

for all $v = (v_1, v_2, \ldots, v_\ell) \in \mathbb{F}_{q^M}^n$ and $w = (w_1, w_2, \ldots, w_\ell) \in \mathbb{F}_{q^M}^n$, where $v_i, w_i \in \mathbb{F}_{q^M}^{n_i}$, for $i = 1, 2, \ldots, \ell$.

The sum-rank metric measures the error and erasure correction capabilities of codes in multishot matrix-multiplicative channels, e.g., multishot network coding [23, 35], space-time coding with multiple fading blocks [16] and local repair with multiple local groups [24].

Not surprisingly, the rank metric is recovered by setting $\ell = 1$, and the classical Hamming metric is recovered by taking $n_1 = n_2 = \ldots = n_\ell = 1$ (or $\ell = n$).

The minimum rank distance of a code $\mathcal{C} \subseteq \mathbb{F}_{q^M}^n$ is defined as

$$d_{\mathrm{R}}(\mathcal{C}) = \min\{d_{\mathrm{R}}(v,w) \mid v, w \in \mathcal{C}, v \neq w\} = \min\{\mathrm{rank}(v) \mid v \in \mathcal{C}, v \neq 0\},$$

and analogously for the sum-rank metric $d_{\mathrm{SR}}(\mathcal{C})$. For an (n,k) code $\mathcal{C} \subseteq \mathbb{F}_{q^M}^n$, a *generator matrix* or *encoder* is a full-rank matrix $G \in \mathbb{F}_{q^M}^{k \times n}$ such that

$$\mathcal{C} = \mathrm{im}_{\mathbb{F}_{q^M}} G = \left\{ uG \;\middle|\; u \in \mathbb{F}_{q^M}^k \right\}.$$

An encoder of $\mathcal{C}$ is called systematic if it is of the form $G = [I_k, P]$, for some matrix $P \in \mathbb{F}_{q^M}^{k \times (n-k)}$, where $I_k \in \mathbb{F}_{q^M}^{k \times k}$ denotes the identity matrix of size k. Note that, by basic linear algebra, any block code has a unique systematic encoder (up to permutation of columns).

For an (n,k) code over $\mathcal{C} \subseteq \mathbb{F}_{q^M}^n$, the analogues of the Singleton bound are given by

$$d_{\mathrm{R}}(\mathcal{C}) \leq \min\left\{1, \frac{M}{n}\right\}(n-k)+1 \quad \text{and} \quad d_{\mathrm{SR}}(\mathcal{C}) \leq \min\left\{1, \frac{\ell M}{n}\right\}(n-k)+1, \tag{2}$$

for the rank and sum-rank metrics, respectively, being the second valid for $n_1 = n_2 = \ldots = n_\ell$. The first was proven in [6], whereas the second was proven in [24].

The bounds in (2) are refinements of the information-theoretical classical bound

$$d_{\mathrm{R}}(\mathcal{C}) \leq n-k+1 \quad \text{and} \quad d_{\mathrm{SR}}(\mathcal{C}) \leq n-k+1, \tag{3}$$

respectively. We will say that $\mathcal{C}$ is MRD (maximum rank distance) or MSRD (maximum sum-rank distance) if it attains the bounds in (3), respectively. The bounds in

(2) imply that MRD codes (resp. MSRD codes) only exist if $M \geq n$ (resp. $M \geq n/\ell$). Note how (2) and (3) coincide for the Hamming metric ($\ell = n$) and the restriction on the extension degree M for the existence of MDS codes vanishes.

Gabidulin codes are a well-known class of MRD codes [6] (see also [10, 30]). It is worth noting that $d_{\mathrm{R}}(\mathcal{C}) \leq d_{\mathrm{SR}}(\mathcal{C})$, thus any MRD code is also MSRD. However, as noted above, MRD codes only exist if $M \geq n$. Linearized Reed-Solomon codes [21] are the only known MSRD codes with subexponential field sizes q^M, and achieve the minimum extension degree $M = n/\ell$ whenever $n_1 = n_2 = \ldots = n_\ell$. Since the fastest decoding algorithms for MRD codes are superlinear in n over $\mathbb{F}_{q^M}$, with $M \geq n$, the known decoding algorithm for linearized Reed-Solomon codes that is quadratic in n over $\mathbb{F}_{q^M}$, with $M = n/\ell$, is more than a degree faster in XOR operations in multishot channels with $\ell \gg 1$ (see [23, Table I]), which are the practical cases (e.g., [16, 24, 23]).

We shall provide necessary and sufficient conditions for a systematic encoder to be MRD. First, we recall a characterization for encoders not necessarily in systematic form. The result is a variant of [6, Theorem 1] and was explicitly presented in [10, Theorem 3.2 and Corollary 3.3] using the Bruhat decomposition for matrices. It is also an immediate consequence of the more general results [20, Theorem 2] or [20, Theorem 6].

Theorem 1 ([10])**.** *Let $G \in \mathbb{F}_{q^M}^{k \times n}$ be an encoder of $\mathcal{C}$. Then, the following statements are equivalent.*

1. *$\mathcal{C}$ is MRD;*
2. *all the full size minors of GA are nonzero for all nonsingular matrices $A \in \mathbb{F}_q^{n \times n}$;*
3. *all the full size minors of GU are nonzero for all nonsingular upper triangular matrices $U \in \mathbb{F}_q^{n \times n}$.*

The main idea behind the proof of condition 3. implies condition 2. above is that every nonsingular matrix A can be written as $A = VQU$ where V and U are upper triangular and Q is a permutation matrix (see, for example, [34]). This decomposition is a consequence of the more general Bruhat decomposition for algebraic groups. Since we use this decomposition frequently throughout the paper, we include its proof below for the sake of completeness.

Lemma 1. *Let $\mathbb{F}$ be a field, let n be a positive integer and let $A \in \mathbb{F}^{n \times n}$ be a nonsingular matrix. Then there exist nonsingular upper triangular matrices $U, V \in \mathbb{F}^{n \times n}$ such that*

$$A = VQU,$$

where Q is a permutation matrix.

Proof. Let $B = P_n A$, where P_n is the permutation matrix with ones in the anti-diagonal. Using Gauss-Jordan elimination we obtain $L^{-1}BU^{-1} = P$, so $B = LPU$, where $L \in \mathbb{F}^{n\times n}$ is a lower triangular matrix, $U \in \mathbb{F}^{n\times n}$ is an upper triangular matrix and P is a permutation matrix. Since $|A| \neq 0$ then L and U are nonsingular. Let $V = P_n L P_n$, then clearly V is nonsingular and upper triangular, also $L = P_n V P_n$. Therefore,

$$A = P_n B = P_n LPU = VQU,$$

where $Q = P_n P$. □

The following result extends Theorem 1 to the sum-rank metric in general. This result was explicitly stated in a more general form in [22, Proposition 7], but was already observed in the proof of [21, Theorem 3].

Theorem 2 ([22])**.** *Let $n = n_1 + n_2 + \cdots + n_\ell$ be a code-length partition defining the sum-rank metric as in (1). Let $G \in \mathbb{F}_{q^M}^{k\times n}$ be an encoder of an (n, k) code $\mathcal{C} \subseteq \mathbb{F}_{q^M}^n$. Then, $\mathcal{C}$ is MSRD if, and only if, all the full size minors of GA are nonzero for all nonsingular block-diagonal matrices*

$$A = \operatorname{diag}(A_1, A_2, \ldots, A_\ell) = \begin{bmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_\ell \end{bmatrix} \in \mathbb{F}_q^{n\times n}, \tag{4}$$

where $A_i \in \mathbb{F}_q^{n_i\times n_i}$, for $i = 1, 2, \ldots, \ell$.

2.2. Convolutional codes

As opposed to block codes, convolutional encoders process an input stream of information bits over a shift register (with possible feedback) and converts it into a stream of transmitted bits. Therefore, they are very suitable for streaming applications [8, 18, 19, 25]. In the sequel, we follow the module-theoretic approach to convolutional codes as it was described in [8, 12, 31, 15, 33]. A *convolutional code* $\mathcal{C}$ of rate k/n, or (n, k) convolutional code, is an $\mathbb{F}_{q^M}[D]$-submodule of $\mathbb{F}_{q^M}^n[D]$ of rank k. A full-row-rank matrix $G(D) \in \mathbb{F}_{q^M}^{k\times n}[D]$ with the property that

$$\mathcal{C} = \operatorname{im}_{\mathbb{F}_{q^M}[D]} G(D) = \left\{ u(D)G(D) \;\mid\; u(D) \in \mathbb{F}_{q^M}^k[D] \right\}$$

is called a *generator matrix* or *encoder* for $\mathcal{C}$. When the code $\mathcal{C}$ admits an encoder in systematic form, *i.e.*, $G(D) = [I_k \;\; P(D)]$, for some $P(D) \in \mathbb{F}_{q^M}^{k\times(n-k)}[D]$, we say that

$\mathcal{C}$ is systematic. Note that, as opposed to block codes, not all convolutional codes admit an encoder in systematic form, not even after column permutation. We will assume that the encoder $G(D)$ is *basic i.e.*, it has a polynomial right inverse.

Write $v(D) = v_0 + v_1 D + \cdots + v_\ell D^\ell \in \mathbb{F}_{q^M}^n[D]$, and represent $G(D)$ as a matrix polynomial,

$$G(D) = G_0 + G_1 D + \cdots + G_m D^m,$$

where $G_m \neq 0$ and $G_i = 0$, for $i > m$. Then we call m the memory of $G(D)$, and for $j = 0, 1, \ldots, m$ we define the code's jth *truncated sliding generator matrix* as

$$G_j^c = \begin{bmatrix} G_0 & G_1 & \cdots & G_j \\ & G_0 & \cdots & G_{j-1} \\ & & \ddots & \vdots \\ & & & G_0 \end{bmatrix}. \tag{5}$$

The truncated codeword can then be represented as

$$v_{[0,j]} = (v_0, v_1, \ldots, v_j) = (u_0, u_1, \ldots, u_j)\ G_j^c \in \mathbb{F}_{q^M}^{(j+1)n}, \tag{6}$$

where, for $t = 0, 1, \ldots, j$, it holds that

$$v_t = \sum_{i=0}^{\ell} u_{t-i} G_i \in \mathbb{F}_{q^M}^n.$$

Observe that, representing truncated codewords in such a way, we may naturally endow them with the sum-rank metric as in the case of block codes. As usual, we will consider the rank metric in each block of n coordinates. Then, for $v(D) = \sum_i v_i D^i \in \mathbb{F}_{q^M}^n[D]$ and $w(D) = \sum_i w_i D^i \in \mathbb{F}_{q^M}^n[D]$, we define as in the previous subsection,

$$d_{\mathrm{SR}}(v_{[0,j]}, w_{[0,j]}) = \sum_{i=0}^{j} d_{\mathrm{R}}(v_i, w_i) = \sum_{i=0}^{j} \mathrm{rank}(M_n(v_i - w_i)),$$

for $j = 0, 1, \ldots$ As usual, we may define $d_{\mathrm{SR}}(v(D), w(D)) = \lim_{j\to\infty} d_{\mathrm{SR}}(v_{[0,j]}, w_{[0,j]})$. As in the block case, each term in the sum corresponds to a shot of a matrix-multiplicative channel, see [26, 19, 35].

For an (n, k) convolutional code $\mathcal{C} \subseteq \mathbb{F}_{q^M}^n[D]$, we define its *free sum-rank distance* as

$$d_{\mathrm{SR}}(\mathcal{C}) = \min\left\{ \sum_{i\geq 0} \mathrm{rank}(v_i) \ \mid \ v(D) \in \mathcal{C}, v(D) \neq 0 \right\},$$

and its jth *column rank distance*, for $j = 0, 1, \ldots$, as

$$d_{\mathrm{SR}}^{j}(\mathcal{C}) = \min\left\{ \sum_{i=0}^{j} \mathrm{rank}(v_i) \;\; | \;\; v(D) \in \mathcal{C}, v_0 \neq 0 \right\}.$$

As the Hamming distance is always larger than or equal to the rank distance, the following upper bound follows from [8, Proposition 2.2] (see also [19, Lemma 1]):

$$d_{\mathrm{SR}}^{j}(\mathcal{C}) \leq (j+1)(n-k)+1. \tag{7}$$

For a systematic (n, k) convolutional code $\mathcal{C}$ with encoder of memory m, it is easy to see that the number $(n-k)(m+1)+1$ is the maximum possible value for the free sum-rank (and Hamming) distance of $\mathcal{C}$.

The codes $\mathcal{C}$ having $d_{\mathrm{SR}}^{j}(\mathcal{C}) = (j+1)(n-k)+1$ for $j = 0, 1, \ldots, m$ will be called *memory Maximum Sum Rank* convolutional codes (m-MSR) (see [19]). In the context of Hamming metric these codes are closely related to the codes called *Optimum Distance Profile* [13, p. 112]. The following result gives necessary and sufficient conditions for a convolutional code to be m-MSR and it was presented in [19, Theorem 3]. First define

$$A_{[0,j]}^{*} = \mathrm{diag}(A_0^{*}, A_1^{*}, \ldots, A_j^{*}) = \begin{bmatrix} A_0^{*} & & & \\ & A_1^{*} & & \\ & & \ddots & \\ & & & A_j^{*} \end{bmatrix}, \tag{8}$$

with $A_i^{*} \in \mathbb{F}_q^{n \times \rho_i}$ matrices, $\rho_i \in \mathbb{N}$ for $i = 0, 1, \ldots, j$.

Theorem 3 ([19])**.** *For $0 \leq i \leq j$, let $0 \leq \rho_i \leq n$ satisfy*

$$\sum_{h=0}^{i} \rho_h \leq k(i+1), \tag{9}$$

for all $i \leq j$ and with equality for $i = j$. The following are equivalent for any convolutional code:

1. $d_{\mathrm{SR}}^{j}(\mathcal{C}) = (j+1)(n-k)+1$*;*
2. *for all full rank $A_{[0,j]}^{*} = \mathrm{diag}(A_0^{*}, A_1^{*}, \ldots, A_j^{*})$ constructed from full rank blocks $A_i^{*} \in \mathbb{F}_q^{n \times \rho_i}$ and ρ_i that satisfy (9), the product $G_j^{c} A_{[0,j]}^{*}$ is nonsingular.*

2.3. Superregular matrices

Superregular matrices have been a fundamental notion in coding theory as they can be used to construct systematic codes with optimal Hamming distance, both block and convolutional codes. Roughly speaking, this is due to the fact that a superregular matrix has the following property: Take any of its rows with Hamming weight, say d. Then, any combination of this row with t other rows yields a vector of Hamming weight $\geq d - t$, see [2, Theorem 3.1]. In this paper, we will show that the notion of superregular matrices can be also used to build codes with maximum rank or sum-rank distances. We will present later some constructions that involves finding a class of superregular matrices with entries in $\mathbb{F}_{q^M}$ that preserve the property of superregularity after some multiplication and addition of matrices in the base field $\mathbb{F}_q$. Next, we formally introduce the notion of superregular matrix.

Let $F = (\mu_{i,j})_{1\leq i,j\leq m} \in \mathbb{F}_{q^M}^{m\times m}$, and let S_m the symmetric group of order m. Recall that the determinant of F is given by

$$|F| = \sum_{\sigma\in S_m} \operatorname{sgn}(\sigma)\mu_{1\sigma(1)}\cdots\mu_{m\sigma(m)}, \tag{10}$$

where the sign of the permutation σ, denoted by $\operatorname{sgn}(\sigma)$, is 1 (resp. -1) if σ can be written as product of an even (resp. odd) number of transpositions. A *trivial term* of the determinant is a term of (10), $\mu_{1\sigma(1)}\cdots\mu_{m\sigma(m)}$, equal to zero. If F is a square submatrix of a matrix B, with entries in $\mathbb{F}_{q^M}$, and all the terms of the determinant of F are trivial we say that $|F|$ is a *trivial minor* of B. We say that B is *superregular* if all its non-trivial minors are different from zero. When a matrix has all its minors nonzero we call it *full superregular*. These matrices have obviously all their entries nonzero and all minors are non-trivial. In that case the classical characterization of MDS block codes follows.

Lemma 2 ([17])**.** *Let $\mathcal{C} = \operatorname{im}_{\mathbb{F}_{q^M}} G \subseteq \mathbb{F}_{q^M}^n$ be an (n, k) block code. Then, $\mathcal{C}$ is MDS if, and only if, all $k \times k$ full size minors of G are nonzero. If G is in systematic form, i.e., $G = [I_k \;\; P]$ for some $P \in \mathbb{F}_{q^M}^{k\times(n-k)}$, then $\mathcal{C}$ is MDS if, and only if, P is full superregular.*

It is important to remark here that there exist several related notions of superregular matrices in the literature. Frequently, see for instance [4], a superregular matrix is defined to be full superregular, e.g., Cauchy matrices. In [17], several examples of triangular matrices were constructed in such a way that all submatrices inside this triangular configuration were nonsingular. However, all these notions do not apply to more general setting, such as the convolutional case, as in this context we need

to consider submatrices that contain zeros. The more recent contributions [8, 9, 12] consider the same notion of superregularity as in this paper (considering minors with zeros), but defined only for lower triangular Toeplitz matrices, see [9] for examples of superregular matrices of size up to 5×5. In [3] *block* Toeplitz superregular matrices were considered for high rate convolutional codes (see also [1, 2]). The advantage of the definition of superregularity considered here is that unifies all existing notions in the literature.

3. Systematic encoders with maximum rank or maximum sum rank distance

In this section, we extend the results that link MDS codes and superregular matrices to the context of rank-metric and sum-rank-metric codes, both block and convolutional. We will see that a code is MRD or MSRD if its systematic encoder with entries in $\mathbb{F}_{q^M}$ is superregular and remains superregular after some operations with matrices that have entries in the base field $\mathbb{F}_q$. We first treat the block case and then address the convolutional counterpart.

3.1. Systematic Encoders of MRD codes

If the encoder is given in systematic form one can derive a characterization in terms only on the parity part of the encoder. This result was obtained independently in [29, Theorem 3.11]. The following proof will be useful for the proof of Theorem 5 in the next subsection.

Theorem 4. *Let $G = [I_k, P] \in \mathbb{F}_{q^M}^{k\times n}$ be a systematic encoder of a rank metric block code $\mathcal{C}$. Then, the following statements are equivalent.*

1. *$\mathcal{C}$ is MRD;*
2. *the matrix*
$$BP\widetilde{A} + C \in \mathbb{F}_{q^M}^{k\times(n-k)}$$
is full superregular, for all $C \in \mathbb{F}_q^{k\times(n-k)}$ and for all nonsingular upper-triangular matrices $B \in \mathbb{F}_q^{k\times k}$ and $\widetilde{A} \in \mathbb{F}_q^{(n-k)\times(n-k)}$.

Proof. (2. $\Rightarrow$ 1.) : Firstly we will prove that if the matrix
$$BP\widetilde{A} + C \in \mathbb{F}_{q^M}^{k\times(n-k)}$$
is full superregular, for all $C \in \mathbb{F}_q^{k\times(n-k)}$ and for all nonsingular upper-triangular matrices $B \in \mathbb{F}_q^{k\times k}$ and $\widetilde{A} \in \mathbb{F}_q^{(n-k)\times(n-k)}$, then all the full size minors of GU are

nonzero for all nonsingular upper triangular matrices $U \in \mathbb{F}_q^{n\times n}$. Hence the result follows from Theorem 1.

Suppose that there exists a $k \times k$ zero minor of GU for a nonsingular upper-triangular $U \in \mathbb{F}_q^{n\times n}$. Write

$$U = \begin{bmatrix} \widetilde{C} & \widehat{C} \\ 0 & \widetilde{A} \end{bmatrix},$$

with $\widetilde{C} \in \mathbb{F}_q^{k\times k}$ and $\widetilde{A} \in \mathbb{F}_q^{(n-k)\times(n-k)}$ nonsingular upper-triangular matrices. Thus,

$$GU = [\widetilde{C} \;\; \widehat{C} + P\widetilde{A}].$$

Denote $B = (\widetilde{C})^{-1} \in \mathbb{F}_q^{k\times k}$, which is a nonsingular upper-triangular matrix. Thus,

$$BGU = [I_n \;\; C + BP\widetilde{A}],$$

where $C = B\widehat{C}$ is a matrix with entries in the base field $\mathbb{F}_q$. As the left multiplication of GU by an invertible matrix B does not change the zeroness of the full size minors of GU, we have that $[I_n \;\; C + BP\widetilde{A}]$ has a zero minor and by Lemma 2, $C + BP\widetilde{A}$ is not full superregular.

$(1. \Rightarrow 2.)$: Suppose that there are a matrix $C \in \mathbb{F}_q^{k\times(n-k)}$ and nonsingular upper-triangular matrices $B \in \mathbb{F}_q^{k\times k}$ and $\widetilde{A} \in \mathbb{F}_q^{(n-k)\times(n-k)}$ such that $C + BP\widetilde{A}$ is not full superregular. Then, there exists a $k \times k$ minor of $[I_k \;\; C + BP\widetilde{A}]$ equal to zero and therefore $B^{-1}[I_k \;\; C + BP\widetilde{A}]$ has a full size zero minor. Thus,

$$B^{-1}[I_k \;\; C + BP\widetilde{A}] = [B^{-1} \;\; B^{-1}C + P\widetilde{A}] = [I_k \;\; P] \begin{bmatrix} B^{-1} & B^{-1}C \\ 0 & \widetilde{A} \end{bmatrix}.$$

Denote

$$U = \begin{bmatrix} B^{-1} & B^{-1}C \\ 0 & \widetilde{A} \end{bmatrix}.$$

It is straightforward to verify that U is nonsingular and upper triangular and GU has a full size zero minor. Taking into consideration the statements of Theorem 1 this concludes the proof. □

3.2. Systematic Encoders of MSRD codes

In this subsection, we will give characterizations for MSRD systematic encoders. The main result (Theorem 5) is an extension of Theorem 4, which can be recovered by setting $\ell = 1$, the case where the sum-rank metric becomes the rank metric.

It is very important to remark that, in contrast with block codes in the rank metric ($\ell = 1$) or Hamming metric ($\ell = n$), the use of a non-trivial code-length partition $n = n_1 + n_2 + \cdots + n_\ell$ implies that we no longer can assume that the identity matrix is placed in the first k coordinates. For full generality, we will need to consider arbitrary partitions $k = k_1 + k_2 + \cdots + k_\ell$ of an information set. This will be transparent in the convolutional case, due to their polynomial nature and the fact that the identity matrix is a constant matrix (see Theorem 6).

Theorem 5. *Let $n = n_1 + n_2 + \cdots + n_\ell$ be a code-length partition defining the sum-rank metric as in (1). Let $k = k_1 + k_2 + \cdots + k_\ell$ be a dimension partition, where $0 \leq k_i \leq n_i$, for $i = 1, 2, \ldots, \ell$. Finally, let*

$$G = [J_1, P_1, J_2, P_2, \ldots, J_\ell, P_\ell] \in \mathbb{F}_{q^M}^{k \times n}$$

be a systematic encoder of an (n, k) code $\mathcal{C} \subseteq \mathbb{F}_{q^M}^n$, where $P_i \in \mathbb{F}_{q^M}^{k \times (n_i - k_i)}$ is arbitrary and where $J_i \in \mathbb{F}_{q^M}^{k \times k_i}$ is zero everywhere except for the i-th block of k_i rows, where it is the identity matrix of size k_i, for $i = 1, 2, \ldots, \ell$. In other words, $I_k = (J_1, J_2, \ldots, J_\ell)$. Denote $P = [P_1, P_2, \ldots, P_\ell] \in \mathbb{F}_{q^M}^{k \times (n-k)}$. Then, the following are equivalent,

1. *$\mathcal{C}$ is MSRD;*
2. *the matrix*

$$\begin{bmatrix} B_1 & & & \\ & B_2 & & \\ & & \ddots & \\ & & & B_\ell \end{bmatrix} P \begin{bmatrix} \widetilde{A}_1 & & & \\ & \widetilde{A}_2 & & \\ & & \ddots & \\ & & & \widetilde{A}_\ell \end{bmatrix} + \begin{bmatrix} C_1 & & & \\ & C_2 & & \\ & & \ddots & \\ & & & C_\ell \end{bmatrix} \in \mathbb{F}_{q^M}^{k \times (n-k)}$$

is full superregular, for all matrices $C_i \in \mathbb{F}_q^{k_i \times (n_i - k_i)}$ and for all nonsingular upper-triangular matrices $B \in \mathbb{F}_q^{k_i \times k_i}$ and $\widetilde{A} \in \mathbb{F}_q^{(n_i - k_i) \times (n_i - k_i)}$, for $i = 1, 2, \ldots, \ell$.

Proof. We may take the matrices A_i in Theorem 2 to be upper triangular. The arguments in this proof will be an extension of those in the proof of Theorem 4. However, we will need to be careful regarding the partition of the information set, which is not an issue in the cases $\ell = 1$ or $\ell = n$, as explained at the beginning of this subsection.

Assume that there exists a $k \times k$ zero minor in GA, for a nonsingular block-diagonal matrix A as in (4), where A_i is upper triangular, for $i = 1, 2, \ldots, \ell$. Write

$$A_i = \begin{bmatrix} \widetilde{C}_i & \widehat{C}_i \\ 0 & \widetilde{A}_i \end{bmatrix} \in \mathbb{F}_q^{n_i \times n_i},$$

where $\widetilde{C}_i \in \mathbb{F}_q^{k_i \times k_i}$, $\widetilde{A}_i \in \mathbb{F}_q^{(n_i-k_i)\times(n_i-k_i)}$ and $\widehat{C}_i \in \mathbb{F}_q^{k_i \times (n_i-k_i)}$, for $i = 1, 2, \ldots, \ell$ (notice that if for some i, $k_i = 0$ then both matrices $\widetilde{C}_i$ and $\widehat{C}_i$ do not exist and if $k_i = n_i$ then both matrices $\widetilde{A}_i$ and $\widehat{C}_i$ do not exist). Now we have that

$$GA = [J_1, P_1, J_2, P_2, \ldots, J_\ell, P_\ell] \begin{bmatrix} \widetilde{C}_1 & \widehat{C}_1 & & & & & & \\ & \widetilde{A}_1 & & & & & & \\ & & \widetilde{C}_2 & \widehat{C}_2 & & & & \\ & & & \widetilde{A}_2 & & & & \\ & & & & \ddots & & & \\ & & & & & & \widetilde{C}_\ell & \widehat{C}_\ell \\ & & & & & & & \widetilde{A}_\ell \end{bmatrix}$$

$$= \begin{bmatrix} \widetilde{C}_1 & \widehat{C}_1 & & & & & \\ & & \widetilde{C}_2 & \widehat{C}_2 & & & \\ & & & & \ddots & & \\ & & & & & \widetilde{C}_\ell & \widehat{C}_\ell \end{bmatrix} + P \begin{bmatrix} 0 & \widetilde{A}_1 & & & & & \\ & & 0 & \widetilde{A}_2 & & & \\ & & & & \ddots & & \\ & & & & & 0 & \widetilde{A}_\ell \end{bmatrix}.$$

Denote $B = \mathrm{diag}((\widetilde{C}_1)^{-1}, (\widetilde{C}_2)^{-1}, \ldots, (\widetilde{C}_\ell)^{-1}) \in \mathbb{F}_q^{k\times k}$, which is nonsingular and upper triangular. Then the reader can check that

$$BGA = [J_1, T_1, J_2, T_2, \ldots, J_\ell, T_\ell] \in \mathbb{F}_{q^M}^{k\times n},$$

where again $I_k = [J_1, J_2, \ldots, J_\ell]$, but now

$$T = [T_1, T_2, \ldots, T_\ell] = BP \begin{bmatrix} \widetilde{A}_1 & & & \\ & \widetilde{A}_2 & & \\ & & \ddots & \\ & & & \widetilde{A}_\ell \end{bmatrix} + \begin{bmatrix} C_1 & & & \\ & C_2 & & \\ & & \ddots & \\ & & & C_\ell \end{bmatrix} \in \mathbb{F}_{q^M}^{k\times(n-k)},$$

where $C_i = \widetilde{C}_i^{-1}\widehat{C}_i \in \mathbb{F}_q^{k_i\times(n_i-k_i)}$, for $i = 1, 2, \ldots, \ell$. As in the proof of Theorem 4, it follows that T is not full superregular.

The reversed implication is proven as in Theorem 4, again taking into account the partition $k = k_1 + k_2 + \cdots + k_\ell$ and the block-diagonal nature of the corresponding matrices. □

It is immediate to see that Theorem 4 is the particular case of Theorem 5 obtained by setting $\ell = 1$. A bit less trivial, but still easy, is to check that the classical characterization of MDS systematic encoders is recovered from Theorem 5 by setting $\ell = n$, or equivalently $n_1 = n_2 = \ldots = n_\ell = 1$. To that end, observe that the block-diagonal matrices $\mathrm{diag}(B_1, B_2, \ldots, B_\ell)$ and $\mathrm{diag}(\widetilde{A}_1, \widetilde{A}_2, \ldots, \widetilde{A}_\ell)$ are nothing but nonsingular diagonal matrices, i.e., monomial matrices. As for $C = \mathrm{diag}(C_0, \ldots, C_m)$ we can assume without loss of generality that the partition of k is $k_i = 1$ for $i \leq k$ and $k_i = 0$ for $k < i \leq n$. So for any $i = 1, \ldots, n$ we have $n_i - k_i = 0$ or $k_i = 0$, so $\widehat{C}_i$ never exists, therefore C does not exist either and we recover the classical characterization of MDS systematic encoders.

3.3. Systematic Encoders of m-MSR convolutional codes

Column distance is arguably the most fundamental distance measure for convolutional codes, [13, pag. 109]. A full characterization of polynomial encoders $G(D)$ that yield codes with optimal column Hamming distance was given in [8] for general encoders and in [7] when the encoder is in systematic form, see also [8, Corollary 2.5]. In this section we provide analogous characterizations in the context of rank metric convolutional codes. We start with a general result about full size minors.

Theorem 6. *Let $\mathcal{C}$ be an $[n, k]$ convolutional code with memory m and a systematic encoder $G(D) = [I_k \quad P(D)]$, where $P(D) = \sum_{i=0}^{m} P_i D^i \in \mathbb{F}_{q^M}^{k\times(n-k)}[D]$, and let $0 \leq j \leq m$. Given $\underline{A}_\ell \in \mathbb{F}_q^{(n-k)\times(n-k)}$, $B_\ell \in \mathbb{F}_q^{k\times k}$ and $C_\ell \in \mathbb{F}_q^{k\times(n-k)}$, with $\ell = 0, 1, \ldots, j$, consider the matrix $T_j = T_j((\underline{A}_\ell, B_\ell, C_\ell)_{\ell=0}^{j})$ defined by*

$$T_j = \begin{bmatrix} B_0 & & & \\ & B_1 & & \\ & & \ddots & \\ & & & B_j \end{bmatrix} \begin{bmatrix} P_0 & P_1 & \cdots & P_j \\ & P_0 & \cdots & P_{j-1} \\ & & \ddots & \vdots \\ & & & P_0 \end{bmatrix} \begin{bmatrix} \underline{A}_0 & \underline{A}_1 & \cdots & \underline{A}_j \\ & \underline{A}_0 & \cdots & \underline{A}_{j-1} \\ & & \ddots & \vdots \\ & & & \underline{A}_0 \end{bmatrix} + \\ + \begin{bmatrix} C_0 & & & \\ & C_1 & & \\ & & \ddots & \\ & & & C_j \end{bmatrix} = \begin{bmatrix} T_{0,0} & T_{0,1} & \cdots & T_{0,j} \\ & T_{1,1} & & \vdots \\ & & \ddots & T_{j-1,j} \\ & & & T_{j,j} \end{bmatrix}. \tag{11}$$

The following statements are equivalent:

1. $d_{\mathrm{SR}}^{j}(\mathcal{C}) = (j+1)(n-k)+1$;

2. *Every square submatrix of T_j with all its diagonal entries in the matrices $T_{s,t}$, where $s,t \in \{0,1,\ldots,j\}$, is nonsingular, for all $C_\ell \in \mathbb{F}_q^{k\times(n-k)}$ and all nonsingular upper triangular matrices $B_\ell \in \mathbb{F}_q^{k\times k}$, $\underline{A}_\ell \in \mathbb{F}_q^{(n-k)\times(n-k)}$;*
3. *T_j is superregular for all $C_\ell \in \mathbb{F}_q^{k\times(n-k)}$ and all nonsingular upper triangular matrices $B_\ell \in \mathbb{F}_q^{k\times k}$, $\underline{A}_\ell \in \mathbb{F}_q^{(n-k)\times(n-k)}$, $\ell = 0,1,\ldots,j$.*

Proof. (2. $\Rightarrow$ 1.) Let $A^*_{[0,j]} = \operatorname{diag}(A^*_0, A^*_1, \ldots, A^*_j)$, where each $A^*_i \in \mathbb{F}_q^{n\times\rho_i}$ is a full rank matrix and $\rho_i \in \mathbb{N}$ is such that $0 \le \rho_i \le n$ and

$$\sum_{h=0}^{i} \rho_h \le k(i+1), \tag{12}$$

for all $i = 0,1,\ldots,j$, with equality in (12) for $i = j$. Since for each $i = 0,1,\ldots,j$, A^*_i has full rank ρ_i, there exists a matrix A'_i such that

$$\breve{A}_i = \begin{bmatrix} A^*_i & A'_i \end{bmatrix} \in \mathbb{F}_q^{n\times n}$$

is nonsingular. Suppose $G^c_j A^*_{[0,j]}$ is singular and consider $\breve{A}_{[0,j]} = \operatorname{diag}(\breve{A}_0, \breve{A}_1, \ldots, \breve{A}_j)$, then

$$G^c_j \breve{A}_{[0,j]} = G^c_j \begin{bmatrix} A^*_0\ A'_0 & & & \\ & A^*_1\ A'_1 & & \\ & & \ddots & \\ & & & A^*_j\ A'_j \end{bmatrix},$$

has a null full size minor as $G^c_j A^*_{[0,j]}$ is a submatrix of it.

Now, by Bruhat decomposition, there exist nonsingular upper triangular matrices A_i and U_i, such that $\breve{A}_i = A_i Q_i U_i$, where Q_i is a permutation. Consider the nonsingular matrices $A_{[0,j]} = \operatorname{diag}(A_0, A_1, \ldots, A_j)$, $U_{[0,j]} = \operatorname{diag}(U_0, U_1, \ldots, U_j)$ and $Q_{[0,j]} = \operatorname{diag}(Q_0, Q_1, \ldots, Q_j)$. Then $\breve{A}_{[0,j]} = A_{[0,j]} Q_{[0,j]} U_{[0,j]}$. Since

$$G^c_j A_{[0,j]} = G^c_j \breve{A}_{[0,j]} U^{-1}_{[0,j]} Q_{[0,j]},$$

then $G^c_j A_{[0,j]}$ has a submatrix $\mathbb{M}$ such that $|\,\mathbb{M}\,| = 0$. Moreover, this matrix is built by selecting ρ_i columns between the $(ik+1)$-th and the $(i+1)k$-th columns of $G^c_j A_{[0,j]}$, $i = 0,1,\ldots,j$ and the ρ_i satisfies (12). Write

$$A_i = \begin{bmatrix} \hat{A}_i & C^*_i \\ & \underline{A}_i \end{bmatrix},$$

where $\hat{A}_i \in \mathbb{F}_q^{k\times k}$ and $\underline{A}_i \in \mathbb{F}_q^{(n-k)\times(n-k)}$ are nonsingular upper triangular matrices.

Therefore,

$$G_j^c A_{[0,j]} = \begin{bmatrix} (I_k \;\; P_0) & (0 \;\; P_1) & \cdots & (0 \;\; P_j) \\ & (I_k \;\; P_0) & & \vdots \\ & & \ddots & \\ & & & (I_k \;\; P_0) \end{bmatrix} \begin{bmatrix} A_0 & & & \\ & A_1 & & \\ & & \ddots & \\ & & & A_j \end{bmatrix}$$

$$= \begin{bmatrix} (\hat{A}_0 \;\; C_0^* + P_0\underline{A}_0) & (0 \;\; P_1\underline{A}_1) & \cdots & (0 \;\; P_j\underline{A}_j) \\ & (\hat{A}_1 \;\; C_1^* + P_0\underline{A}_0) & & \vdots \\ & & \ddots & \\ & & & (\hat{A}_1 \;\; C_j^* + P_j\underline{A}_j) \end{bmatrix}.$$

Let $B_i = (\hat{A}_i)^{-1} \in \mathbb{F}_q^{k\times k}$ and $B_{[0,j]} = \mathrm{diag}(B_0, B_1, \ldots, B_j)$. Then

$$B_{[0,j]} G_j^c A_{[0,j]} = \begin{bmatrix} (I_k \;\; C_0 + B_0P_0\underline{A}_0) & (0 \;\; B_0P_1\underline{A}_1) & \cdots & (0 \;\; B_0P_j\underline{A}_j) \\ & (I_k \;\; C_1 + B_1P_0\underline{A}_1) & & \vdots \\ & & \ddots & \\ & & & (I_k \;\; C_j + B_jP_0\underline{A}_j) \end{bmatrix},$$

where $C_i = B_iC_i^*$. Let $\rho_i = \mathfrak{I}_i + \mathfrak{T}_i$ where $\mathfrak{T}_i$ corresponds to the number of columns of $B_{[0,j]}\mathbb{M}$ selected from the block columns starting with $B_0P_i\underline{A}_i$ and $\mathfrak{I}_i$ corresponds to number of columns of $B_{[0,j]}\mathbb{M}$ selected from the block columns containing the identity matrix I_k in the i-th block position.

After permutation of columns, which again do not change the zeroness of the full minors, we obtain

$$\begin{bmatrix} & \underbrace{\begin{bmatrix} C_0 + B_0P_0\underline{A}_0 & B_0P_1\underline{A}_1 & & B_0P_j\underline{A}_j \\ & C_1 + B_1P_0\underline{A}_1 & & \\ & & \ddots & \\ & & & C_j + B_jP_0\underline{A}_j \end{bmatrix}}_{=T_j} \\ I_{k(j+1)} & \end{bmatrix}. \tag{13}$$

We are going to prove that there exists a unique square submatrix of T_j, say M, such that $|\,M\,| = 0$ and its diagonal entries are in the matrices $T_{s,t}$, where $s, t \in \{0, 1, \ldots, j\}$.

Let $\hat{\mathbb{M}}$ be the matrix that corresponds to $B_{[0,j]}\mathbb{M}$ after the change of columns, $S_j = \mathfrak{I}_0 + \mathfrak{I}_1 + \cdots + \mathfrak{I}_j$ and denote by $c_1, c_2, \ldots, c_{S_j}$ the indices of the columns of $\hat{\mathbb{M}}$ selected in the first $k(j+1)$ positions of (13), and $c_{S_j+1}, \ldots, c_{(j+1)k}$ the indices from the remaining columns of $\hat{\mathbb{M}}$. Let M be the square submatrix of T_j, built by selecting the columns indexed by $c_{S_j+1}, \ldots, c_{(j+1)k}$ and the rows indexed in $\{1, 2, \ldots, (j+1)k\} \setminus \{c_1, c_2, \ldots, c_{S_j}\}$. Therefore,

$$0 = |\,\hat{\mathbb{M}}\,| = \pm |\,M\,|$$

by the Laplace expansion over each of the first S_j columns of $\hat{\mathbb{M}}$.

It remains to show that all the diagonal entries of M are in the matrices $T_{s,t}$, where $s, t \in \{0, 1, \ldots, j\}$, which we will achieve using the index condition (12) on the submatrix $\hat{\mathbb{M}}$. Recall that $\rho_i = \mathfrak{I}_i + \mathfrak{T}_i$ and write

$$M = \left[\begin{array}{c|c|c|c} M_0 & & & \\ \hline & M_1 & & \\ O_0 & \hline & \cdots & \\ & O_1 & & M_{j-1} \\ & & & \hline & M_j \\ & & & O_{j-1} & \end{array}\right], \tag{14}$$

with M_i having $\mathfrak{T}_i$ columns and $k(i+1) - \sum_{h=0}^{i} \mathfrak{I}_h$ rows, $i = 0, 1, \ldots, j$. Having all the entries of the diagonal of M in the matrices $T_{s,t}$ amounts to saying that the number of rows of each M_i is larger or equal to $\sum_{h=0}^{i} \mathfrak{T}_h$, *i.e.*,

$$k(i+1) - \sum_{h=0}^{i} \mathfrak{I}_h \geq \sum_{h=0}^{i} \mathfrak{T}_h,$$

for $i = 0, 1, \ldots, j$. But these are exactly the conditions (12). This shows (2. $\Rightarrow$ 1.).

(1. $\Rightarrow$ 2.) For the converse, let M be a square singular submatrix of T_j of order ν, where $\nu \leq \min\{(j+1)k, (j+1)(n-k)\}$, with its diagonal entries in the matrices $T_{s,t}$, where $s, t \in \{0, 1, \ldots, j\}$. Suppose that M is formed by the columns $d_1, \ldots, d_\nu$ and rows $c_1, \ldots, c_\nu$ of T_j. Clearly, M can be written in the form (14). Let $\mathfrak{T}_i$ be the number of columns of the matrix M_i and let $\mathfrak{I}_i$ be such that the number of rows in M_i is $k(i+1) - \sum_{h=0}^{i} \mathfrak{I}_h$. The condition on the entries of M implies that

$$k(i+1) \geq \sum_{h=0}^{i} \mathfrak{I}_h + \sum_{h=0}^{i} \mathfrak{T}_h,$$

Let $\rho_i = \mathfrak{I}_i + \mathfrak{T}_i$. Then the ρ_i satisfy the conditions (12). Let $\hat{\mathbb{M}}$ be the submatrix of the matrix $[I_{(j+1)k} \mid T_j]$ formed by the columns indexed in $\{1, 2, \ldots, (j+1)k\} \setminus$

$\{c_1, c_2, \ldots, c_\nu\}$ and the columns $d_1, \ldots, d_\nu$ of T_j, and all of the $(j+1)k$ rows. Then, by the Laplace expansion over each of its columns $\{1, 2, \ldots, (j+1)k\} \setminus \{c_1, c_2, \ldots, c_\nu\}$ $|\,\hat{\mathbb{M}}\,| = \pm|\,M\,| = 0$.

If we write $C_i^* = C_i B_i^{-1}$, $\hat{A}_i = B_i^{-1}$,

$$A_i = \begin{bmatrix} \hat{A}_i & C_i^* \\ & \underline{A}_i \end{bmatrix}$$

and $A_{[0,j]} = \mathrm{diag}(A_0, A_1, \ldots, A_j)$, then after a permutation of columns, $\hat{\mathbb{M}}$ corresponds to a submatrix, say $\mathbb{M}$, of $G_j^c A_{[0,j]}$ satisfying conditions (12). It is easy to see that this submatrix of $G_j^c A_{[0,j]}$ is equal to $G_j^c A_{[0,j]}^*$ for $A_i^* \in \mathbb{F}_q^{n \times \rho_i}$ and ρ_i satisfying condition (12). Hence, if M is singular, then $G_j^c A_{[0,j]}^*$ is also singular, and by Theorem 3 statement 1. fails to hold. Therefore (1. $\Rightarrow$ 2.).

The equivalence (2. $\Leftrightarrow$ 3.) readily follows from the fact that if there is a zero in the diagonal, all the entries to the right and below are also zero and therefore the determinant of such matrix is trivially zero. □

Observation 1. *Notice that condition 2. implies that all the entries of the matrices $T_{s,t}$, where $s, t \in \{0, 1, \ldots, j\}$ are nonzero.*

3.4. General Convolutional Encoders

If the convolutional code is not systematic one can easily transform the sliding generator matrix of a nonsystematic encoder in order to apply the conditions of Theorem 6. This fact is straightforward but worth mentioning.

Let $G(D) = [S(D) \;\; Q(D)]$ be the generator matrix of $\mathcal{C}$, where

$$S(D) = \sum_{i=0}^{m} S_i D^i \in \mathbb{F}_{q^M}^{k \times k}[D],$$

$$Q(D) = \sum_{i=0}^{m} Q_i D^i \in \mathbb{F}_{q^M}^{k \times (n-k)}[D].$$

As $\mathcal{C}$ is basic, we can assume without loss of generality that $S_0 = I_k$, the identity matrix of size k. Further, let

$$S^{-1}(D)Q(D) = \sum_{i=0}^{\infty} P_i D^i \in \mathbb{F}^{k \times (n-k)}(\!(D)\!) \tag{15}$$

be the Laurent expansion of $S^{-1}(D)Q(D)$ over the field $\mathbb{F}(\!(D)\!)$ of Laurent series.

It is easy to see that, after a column permutation, the sliding parity-check matrix G_j^c, $j = 0, 1, \ldots m$ of $\mathcal{C}$ has the form

$$G_j^c = \left(\begin{bmatrix} S_0 & S_1 & \cdots & S_j \\ & S_0 & \cdots & S_{j-1} \\ & & \ddots & \vdots \\ & & & S_0 \end{bmatrix} \middle| \begin{bmatrix} Q_0 & Q_1 & \cdots & Q_j \\ & Q_0 & \cdots & Q_{j-1} \\ & & \ddots & \vdots \\ & & & Q_0 \end{bmatrix} \right)$$

and using that $S_0 = I_k$ we can left multiply G_j^c by the inverse of the first block to obtain

$$\left(I_{k(j+1)} \middle| \begin{bmatrix} P_0 & P_1 & \cdots & P_j \\ & P_0 & \cdots & P_{j-1} \\ & & \ddots & \vdots \\ & & & P_0 \end{bmatrix} \right) \tag{16}$$

As these operations do not change the full size minors of G_j^c one can use the representation (16) and Theorem 6 and check whether $d_{\text{SR}}^j(\mathcal{C}) = (j+1)(n-k)+1$ or not.

We have considered in this paper $j \leq m$ but we note that non-systematic convolutional codes have column distances that grow to a time instant that can be larger than m, namely, $L = \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor$, where δ is the *degree* of the convolutional code defined to be the maximum of the degrees of the determinants of the $k \times k$ sub-matrices of one, and hence any, generator matrix of $\mathcal{C}$, see [33] for details.

4. Reducing the field size of m-MSR codes

In [19] a general construction of m-MSR convolutional codes was presented. Unfortunately, we were unable to find a general construction of superregular matrices that satisfy the conditions of Theorem 6. We conjecture, based on many examples, that the superregular matrices proposed in [1, 2, 19], and presented below, satisfy such conditions and therefore can be used to build systematic m-MSR convolutional codes, but we were unable to formally prove it.

In any case, the main problem of all these general constructions is that they require impractically large finite fields. For this reason, most of the optimal constructions of convolutional codes presented over finite fields of reasonable size are found via computer search and limited to small parameters, see for instance [3, 8, 9, 12]. In this section we present concrete examples of superregular matrices, of given parameters and finite fields, that satisfy conditions of Theorem 6 and therefore yield m-MSR convolutional codes. The examples presented in [19] were built requiring

$[n,k,m]$	Achievable field	# non-trivial minors	# Matrices $\underline{A}_\ell$ and B_ℓ	Achievable field in [19]
$[2,1,1]$	$\mathbb{F}_{2^2}$	1	1×1	$\mathbb{F}_{2^5}$
$[2,1,2]$	$\mathbb{F}_{2^3}$	7	1×1	$\mathbb{F}_{2^7}$
$[3,2,1]$	$\mathbb{F}_{2^4}$	5	1×4	
$[3,1,1]$	$\mathbb{F}_{2^5}$	6	4×1	
$[4,2,1]$	$\mathbb{F}_{2^6}$	40	4×4	$\mathbb{F}_{2^{11}}$
$[3,2,2]$	$\mathbb{F}_{2^7}$	42	1×8	$\mathbb{F}_{2^{11}}$
$[3,1,2]$	$\mathbb{F}_{2^9}$	42	8×1	$\mathbb{F}_{2^{11}}$
$[4,2,2]$	$\mathbb{F}_{2^{11}}$	529	8×8	
$[5,3,1]$	$\mathbb{F}_{2^{11}}$	136	4×64	
$[5,2,1]$	$\mathbb{F}_{2^{12}}$	136	64×4	
$[6,4,1]$	$\mathbb{F}_{2^{13}}$	335	4×4096	
$[6,2,1]$	$\mathbb{F}_{2^{14}}$	670	4096×4	
$[6,3,1]$	$\mathbb{F}_{2^{18}}$	634	64×64	

Table 1: Parameters of m-MSR convolutional codes obtained by computer search.

that G_j^c is superregular and remains superregular after certain operations over $\mathbb{F}_q$ whereas in our constructions we only need that the smaller matrix P_j^c is superregular and remains superregular after certain operations over $\mathbb{F}_q$. Therefore, the field sizes obtained improve the ones presented in [19], as Table 1 shows. The examples are built using the following superregular matrices.

Let α be a primitive element of a finite field $\mathbb{F}_{q^M}$ with q^M elements and consider $G(D)=[I_k \;\; P(D)]$ with $P(D)=\sum_{i=0}^{m} P_i D^i$ where P_i, for $0\leq i\leq m$ is equal to

$$P_i=\begin{bmatrix} \alpha^{[Ri]} & \alpha^{[Ri+1]} & \cdots & \alpha^{[Ri+n-k-1]} \\ \alpha^{[Ri+1]} & \alpha^{[Ri+2]} & \cdots & \alpha^{[Ri+n-k]} \\ \alpha^{[Ri+2]} & \alpha^{[Ri+3]} & \cdots & \alpha^{[Ri+n-k+1]} \\ \vdots & \vdots & \vdots & \\ \alpha^{[Ri+k-1]} & \alpha^{[Ri+k]} & \cdots & \alpha^{[Ri+n-2]} \end{bmatrix} \in \mathbb{F}_{q^M}^{k\times(n-k)}, \tag{17}$$

where $R=\max\{k,n-k\}$ and where we use the notation $\alpha^{[j]}=\alpha^{q^j}$ to denote the

j-th Frobenius power of $\alpha \in \mathbb{F}_{q^M}$. The next matrix

$$P_j^c = \begin{bmatrix} P_0 & P_1 & \cdots & P_j \\ & P_0 & \cdots & P_{j-1} \\ & & \ddots & \vdots \\ & & & P_0 \end{bmatrix} \tag{18}$$

is superregular for all $j \leq m$ if the field size is sufficiently large, see [1] for details. For smaller fields it may not be superregular. Nevertheless, for the parameters $[n, k, m]$ and field size displayed in Table 1, this matrix satisfies the conditions of Theorem 6 and can be used to construct m-MSR convolutional codes.

Table 1 shows the achievable fields obtained by computation. For all possible matrices $\underline{A}_\ell$ and B_ℓ (with $\ell = 0, \ldots, m$), all the non-trivial minors of $T_m - C$, are not in the base field $\mathbb{F}_2$, where $C = \text{diag}(C_0, \ldots, C_m)$, which implies that all the non-trivial minors of T_m are nonzero. For this reason we did not consider any matrix C in our calculations and therefore optimize our algorithms.

Another possibility in the quest to find optimal constructions of convolutional codes over small fields is to relax the condition of maximum (sum) rank distance and use instead the notion of almost MRD, see [5]. This is left for future research.

Acknowledgement

The first author is partially supported by the Portuguese Foundation for Science and Technology (FCT-Fundação para a Ciência e a Tecnologia), through CIDMA - Center for Research and Development in Mathematics and Applications, within project UID/MAT/04106/2019. The second listed author gratefully acknowledges the support from The Independent Research Fund Denmark (Grant No. DFF-7027-00053B). The third author is partially supported by the the Universitat d'Alacant (Grant No. VIGROB-287) and Generalitat Valenciana (Grant No. AICO/2017/128).

[1] Almeida, P., Napp, D., Pinto, R., 2013. A new class of superregular matrices and MDP convolutional codes. Linear Algebra and its Applications 439 (7), 2145–2157.

[2] Almeida, P., Napp, D., Pinto, R., 2016. Superregular matrices and applications to convolutional codes. Linear Algebra and its Applications 499, 1–25.

[3] Barbero, A., Ytrehus, Ø., 2018. Rate $(n-1)/n$ systematic memory maximum distance separable convolutional codes. IEEE Trans. Inform. Theory 64 (4), 3018–3030.

[4] Blaum, M., Roth, R. M., 1999. On lowest density MDS codes. IEEE Trans. Inform. Theory 45 (1), 46–59.

[5] de la Cruz, J., 2018. On dually almost MRD codes. Finite Fields and Their Applications 53, 1 – 20.

[6] Gabidulin, É., 1985. Theory of codes with maximum rank distance. Probl. Inf. Transm. 21, 1–12.

[7] Gabidulin, É., 1988. Convolutional codes over large alphabets. Proc. Int. Workshop on Algebraic Combinatorial and Coding Theory, Varna, Bulgaria, 80–84.

[8] Gluesing-Luerssen, H., Rosenthal, J., Smarandache, R., 2006. Strongly MDS convolutional codes. IEEE Trans. Inform. Theory 52 (2), 584–598.

[9] Hansen, J., Østergaard, J., Kudahl, J., Madsen, J. H., 2017. Superregular lower triangular Toeplitz matrices for low delay wireless streaming. IEEE Transactions on Communications 65 (9), 4027–4038.

[10] Horlemann-Trautmann, A., Marshall, K., 2017. New criteria for MRD and Gabidulin codes and some rank-metric code constructions. Advances in Mathematics of Communications 11 (3), 533–548.

[11] Horlemann-Trautmann, A.-L., Marshall, K., Rosenthal, J., 2018. Extension of overbeck's attack for gabidulin-based cryptosystems. Designs, Codes and Cryptography 86 (2), 319–340.

[12] Hutchinson, R., Smarandache, R., Trumpf, J., 2008. On superregular matrices and MDP convolutional codes. Linear Algebra and its Applications 428, 2585–2596.

[13] Johannesson, R., Zigangirov, K. S., 2015. Fundamentals of Convolutional Coding. IEEE Press, New York.

[14] Kötter, R., Kschischang, F., Aug 2008. Coding for errors and erasures in random network coding. IEEE Trans. Inform. Theory 54 (8), 3579–3591.

[15] Lieb, J., 2019. Complete MDP convolutional codes. Journal of Algebra and Its Applications 18 (06), 1950105.

[16] Lu, H.-F., Kumar, P. V., May 2005. A unified construction of space-time codes with optimal rate-diversity tradeoff. IEEE Trans. Inform. Theory 51 (5), 1709–1730.

[17] MacWilliams, F. J., Sloane, N. J., 1977. The Theory of Error-Correcting Codes. North Holland, Amsterdam.

[18] Mahmood, R., Badr, A., Khisti, A., 2015. Streaming-codes for multicast over burst erasure channels. IEEE Trans. Inform. Theory 61 (8), 4181–4208.

[19] Mahmood, R., Badr, A., Khisti, A., 2016. Convolutional codes with maximum column sum rank for network streaming. IEEE Trans. Inform. Theory 62 (6), 3039–3052.

[20] Martínez-Peñas, U., July 2016. On the similarities between generalized rank and Hamming weights and their applications to network coding. IEEE Trans. Inform. Theory 62 (7), 4081–4095.

[21] Martínez-Peñas, U., 2018. Skew and linearized Reed–Solomon codes and maximum sum rank distance codes over any division ring. Journal of Algebra 504, 587 – 612.

[22] Martínez-Peñas, U., 2019. Theory of supports for linear codes endowed with the sum-rank metric. Designs, Codes and Cryptography 87(10), 2295 –2320.

[23] Martínez-Peñas, U., Kschischang, F. R., Aug 2019. Reliable and secure multishot network coding using linearized Reed-Solomon codes. IEEE Trans. Inform. Theory 65 (8), 4785–4803.

[24] Martínez-Peñas, U., Kschischang, F. R., 2019. Universal and dynamic locally repairable codes with maximal recoverability via sum-rank codes. IEEE Transactions on Information Theory, 1–1.

[25] McEliece, R. J., 1998. The algebraic theory of convolutional codes. In: Handbook of Coding Theory. Vol. 1. Elsevier Science Publishers, pp. 1065–1138.

[26] Napp, D., Pinto, R., Rosenthal, J., Vettori, P., 2017. MRD rank metric convolutional codes. IEEE International Symposium on Information Theory (ISIT) 2017, 2766–2770.

[27] Napp, D., Smarandache, R., 2016. Constructing strongly MDS convolutional codes with maximum distance profile. Advances in Mathematics of Communications 10 (2), 275–290.

[28] Neri, A., 2018. Systematic encoders for generalized Gabidulin codes and the q-analogue of Cauchy matrices. CoRR abs/1805.06706.
URL `http://arxiv.org/abs/1805.06706`

[29] Neri, A., July 2019. Algebraic Theory of Rank-Metric Codes: Representations, Invariants and Density Results. PhD thesis. University of Zurich, Switzerland.

[30] Otal, K., Özbudak, F., 2018. Some new non-additive maximum rank distance codes. Finite Fields and Their Applications 50, 293 – 303.

[31] Oued, M. E., Napp, D., Pinto, R., Toste, M., 2019. On duals and parity-checks of convolutional codes over $\mathbb{Z}_{p^r}$. Finite Fields and Their Applications 55, 1 – 20.

[32] Rawat, A. S., Koyluoglu, O. O., Silberstein, N., Vishwanath, S., 2014. Optimal locally repairable and secure codes for distributed storage systems. IEEE Transactions on Information Theory 60 (1), 212–236.

[33] Rosenthal, J., Smarandache, R., 1999. Maximum distance separable convolutional codes. Appl. Algebra Engrg. Comm. Comput. 10 (1), 15–32.

[34] Tyrtyshnikov, E., 1997. Matrix Bruhat decompositions with a remark on the QR (GR) algorithm. Linear Algebra and its Applications 250, 61 – 68.

[35] Wachter-Zeh, A., Stinner, M., Sidorenko, V., June 2015. Convolutional codes in rank metric with application to random network coding. IEEE Trans. Inform. Theory 61 (6), 3199–3213.